Делимость на попарно взаимно простые числа

- $8, 15$ — не простые, но взаимно простые.
- $6, 8, 9$ — взаимно простые (в совокупности) числа, но не попарно простые.
- $8, 15, 49$ — попарно простые и взаимно простые (в совокупности).

Попарно взаимно простые – любые два из множества взаимно просты

m = произведение таких чисел $m_1 \ldots m_k$

Лемма 7

Пусть $m_1, \ldots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \ldots m_k$. Пусть $b \in \mathbb{Z}$ таково, что $b \vdots m_1, \ldots, b \vdots m_k$. Тогда $b \vdots m$.

Доказательство. Пусть $n_\ell = m_1 \ldots m_\ell$. Докажем индукцией по ℓ, что $b \vdots n_\ell$.

- **База** $\ell = 1$ очевидна.

Действительно очевидно

Переход $\ell \to \ell + 1$. • По индукционному предположению $b = cn_\ell$, где $c \in \mathbb{Z}$.

- Так как $cn_\ell = b \vdots m_{\ell+1}$ и $(n_\ell, m_{\ell+1}) = 1$, по Свойству 3 взаимно простых чисел имеем $c \vdots m_{\ell+1}$.
- Тогда $c = dm_{\ell+1}$ и $b = dm_{\ell+1}n_\ell = dn_{\ell+1}$.

Если $b \vdots n_l$ => $b = cn_l$

По индукции:
$cn_l = b \vdots m_{l+1}$ и очев $(n_l, m_{l+1}) = 1$
по свойству $(a,b) = 1$ и $ac \vdots b$ => $c \vdots b$
в нашем случае имеем:
$(n_l, m_{l+1}) = 1$ и $cn_l \vdots m_{l+1}$ => $c \vdots m_{l+1}$

Тогда представим $c = dn_l$ и
$b = dn_l\, m_{l+1} = dn_{l+1}$
(мы просто добавили в произведение эдемент m_{l+1} => все произведение теперь n_{l+1})

Китайская теорема об остатках

Определение

Пусть $m \in \mathbb{N}$; $a, b \in \mathbb{Z}$. Будем говорить, что a **сравнимо** с b по модулю m, если $a - b \vdots m$. Обозначения: $a \equiv_m b$ или $a \equiv b \pmod{m}$.

Теорема 19

Пусть $m_1, \dots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \dots m_k$, $a_1, \dots, a_k \in \mathbb{Z}$. Тогда существует единственное такое $a \in \{0, 1, \dots, m-1\}$, что $a \equiv_{m_1} a_1$, ..., $a \equiv_{m_k} a_k$.

Доказательство. $\exists$. • Пусть $n_\ell = m_1 \dots m_\ell$. Докажем индукцией по ℓ существование такого $b_\ell \in \mathbb{Z}$, что $b_\ell \equiv_{m_1} a_1$, ..., $b_\ell \equiv_{m_\ell} a_\ell$.

База $\ell = 1$ очевидна.

Реально: b ≡ a (mod m), всегда ∃ b: b – a ⋮ m

ПСВ – дают разные остатки по модулю

Переход $\ell \to \ell + 1$. • Так как $(m_{\ell+1}, n_\ell) = 1$ по Теореме 13 числа b_ℓ, $b_\ell + n_\ell$, $b_\ell + 2n_\ell$, ..., $b_\ell + (m_{\ell+1} - 1)n_\ell$ — ПСВ $\pmod{m_{\ell+1}}$ (они получены из ПСВ 0,1, ..., $m_{\ell+1} - 1$ умножением на n_ℓ и прибавлением b_ℓ).

Теорема 13

Пусть $a_1, \dots, a_m$ — ПСВ $\pmod{m}$, $k, b \in \mathbb{Z}$, причем $(k, m) = 1$. Тогда $ka_1 + b, \dots, ka_m + b$ — ПСВ $\pmod{m}$.

Доказательство. • Достаточно проверить критерий из Леммы 2.

• Пусть $ka_i + b \equiv_m ka_j + b \iff k(a_i - a_j) \vdots m$.

• Так как $(k, m) = 1$, это означает, что $a_i - a_j \vdots m \iff a_i \equiv_m a_j$, что не так.

• Значит, среди этих чисел есть число $kn_\ell + b_\ell \equiv_{m_{\ell+1}} a_{\ell+1}$. Положим $b_{\ell+1} := kn_\ell + b_\ell$.

• Тогда $b_{\ell+1} - a_{\ell+1} \vdots m_{\ell+1}$.

• По построению $b_{\ell+1} - b_\ell \vdots n_\ell$. Так как по индукционному предположению $b_\ell - a_i \vdots m_i$ для всех $i \in \{1, \dots, \ell\}$, мы имеем $b_{\ell+1} - a_i = (b_{\ell+1} - b_\ell) + (b_\ell - a_i) \vdots m_i$.

• Итак, мы получили число b_k, удовлетворяющее всем требованиям теоремы, кроме одного: число должно быть от 0 до $m - 1$.

• Для получения такого числа a поделим b_k с остатком на m: пусть $b_k = mq + a$, $0 \le a \le m - 1$.

• Так как $a - b_k \vdots m \vdots m_i$ и $b_k - a_i \vdots m_i$, то и $a - a_i \vdots m_i$ для всех $i \in \{1, \dots, k\}$.

! • Предположим, что a и a' — два различных числа, удовлетворяющих условию. Тогда $a - a' \vdots m_i$ для всех $i \in \{1, \dots, k\}$.

• Так как $m_1, \dots, m_k$ попарно взаимно просты, по Лемме 7 $a - a' \vdots m = m_1 \dots m_k$. Но $|a - a'| < m$, противоречие. $\square$

Лемма 7

Пусть $m_1, \dots, m_k$ — попарно взаимно простые натуральные числа, $m = m_1 \dots m_k$. Пусть $b \in \mathbb{Z}$ тако... что $b \vdots m_1$, ..., $b \vdots m_k$. Тогда $b \vdots m$.

• Из доказательства единственности в Теореме 19 видно, что все целые числа a, для которых $a - a_i \vdots m_i$ при всех $i \in \{1, \dots, k\}$ образуют в точности один вычет по модулю $m = m_1 \dots m_k$.